一种新型基于格上 LWE 问题密钥交换协议的设计 *

李子臣 [1,2]，谢　婷 [1,3]，张筱薇 [3]，蔡居良 [3]

(1. 西安电子科技大学 通信工程学院，西安 710071; 2. 北京印刷学院，北京 102600; 3. 北京电子科技学院，北京 100070)

摘　要：基于格上困难问题设计高效、安全的后量子密钥交换协议具有非常重要的理论意义和实用价值。提出了一种新型高效实用的基于格上错误学习问题被动安全密钥交换协议。该协议采用加密机制的构造方式并使用了密文压缩技术，与 2016 年 Bos 等人基于错误学习问题并使用 Peikert 错误调和机制设计的密钥交换协议 Frodo 相比，通信量只增加了 1.09%，但方案复杂度有效降低，计算更加简洁高效，且协议在被动攻击下可证明安全，可有效抵御量子攻击。该协议与现有的基于错误学习问题设计的密钥交换协议相比，具有很强的竞争力。

关键词：格；密钥交换协议；错误学习问题；被动安全

中图分类号：TP301.4　　doi: 10.3969/j.issn.1001-3695.2017.11.0755

New key exchange protocol of based on LWE problem

Li Zichen[1,2], Xie Ting [1,3], Zhang Xiaowei[3], Cai Juliang[3]

(1. *Communication Engineering Institute*, *Xidian University*, *Xi'an* 710071 *China*; 2. *Beijing Institute of Graphic Communication*, *Beijing* 102600 *China*; 3. *Beijing Electronic Science and Technology Institute*, *Beijing* 100070 *China*)

Abstract: The design of efficient and secure lattice-based post quantum key exchange protocols has certain practical and theoretical significance. In this paper, a scheme was proposed, which used straight-forward transformation LWE encryption mechanism and a ciphertext compression technology. This is a passively secure and practical key exchange protocol. Frodo was a key exchange scheme based on LWE problem proposed by Bos et al, which used the error reconciliation mechanism proposed by Peikert. The main advantage of the scheme over Frodo is simplicity. Compared with Frodo, the communications traffic merely increased by only 1.09%, the complexity of the scheme is reduced effectively. The scheme is proved to be passive security, Also, which can resist quantum computer attacks. Compared with existing key exchange protocol based on learning with error, this protocol is very competitive.

Key Words: lattice; key exchange protocol; LWE; passively secure

chinaXiv:201804.02040v1

0　引言

密钥交换协议[1,2]在安全通信领域中具有重要的基础性作用，它使得两方或多方通过在公开信道上交换信息达成一个共享的会话密钥，被认为是公钥密码学中的一个重要应用。1976 年，Diffie-Hellman 提出了第一个密钥交换协议[3]，自 DH 密钥交换协议提出以来，由于它的构造结构简单且实用，因此之后很多密码学者以此结构为基础来构造高效的密钥交换协议。随着量子计算技术的飞速发展，基于经典的数论困难问题构造的传统公钥密码算法的安全性面临现实威胁。美国国家标准和技术研究院(NIST)于 2015 年颁布的后量子密码学报告[4]中指出：由于量子计算技术的迅速发展，现有的公钥密码标准将不再安全。美国国家标准和技术研究院（NIST）、美国国家安全局（NSA）、以及由欧盟赞助的 PQCRYPTO 项目目前已经在全球范围内展开了后量子密码算法标准的有关征集工作。量子计算机环境下可证明安全的公钥密码算法的研究已成为当前密码学界的热点。其中，后量子密钥交换协议的需求最为迫切，已被美国国家标准和技术研究院（NIST）列为一项重大科研项目。因此设计高效安全的后量子密钥交换协议具有重要的理论意义和应用价值。

基于格理论的密码系统具有较高的渐进效率、可并行计算、可抵御量子攻击等优点，因此格理论被公认为后量子密码算法标准最有力的竞争者。近年来，基于格理论在构造加密[5-7]、数字签名[8,9]、密钥交换[10~15]具有可证明安全性方案以及基于格的

基金项目：国家自然科学基金资助项目（61370188）；北京市支持中央高校共建项目—青年英才计划；中央高校基本科研业务费专项资金资助项目

作者简介：李子臣（1965–），河南焦作人，博导.主要研究方向为公钥密码学、信息安全、后量子签名理论、云计算（1174015268@qq.com）；谢婷（1991-），女，河南鹤壁人，硕士研究生，主要研究方向为格理论公钥密码学、信息安全；张筱薇（1995-），女，河北衡水人，硕士研究生，主要研究方向为无线通信安全、密码学.蔡居良（1993-），男，河南郑州人，硕士研究生，主要研究方向为无线通信安全、密码学.

chinaXiv:201804.02040v1

零知识研究[16]等方面取得了大量研究成果。2005 年 Regev 等人提出带误差的学习问题（learning with errors，LWE）[17]，并指出可使用量子规约技术将 LWE 问题的平均情形困难性和格上的困难问题的最坏情形困难性联系起来。2010 年，Lyubashevsky，Peikert 和 Regev 提出了基于环带误差的学习问题[18]（ring learning with errors，RLWE），显著改进了密钥长度的大小并有效提升了执行的效率。2015 年，Langlois 和 Stele 研究了模 LWE[19]，它是 LWE 与 RLWE 的推广。基于 LWE、RLWE、模 LWE 在密钥交换协议的构造方面已经得到了广泛应用。

近几年来在基于格困难问题构造被动安全的密钥交换协议方面，出现了许多优秀的成果。起初，2012 年丁等人首次提出一种基于 LWE 变体 SLWE 的密钥交换协议[10]，并将该方案扩展到 RLWE 上。2014 年，Peikert 首先提出了一种高效的选择明文安全的密钥封装机制及一种有效但计算复杂的错误调和机制构造认证密钥交换协议[11]。在 2015 年，Bos 等人在 S&P 会议上提出一种 Diffie-Hellman 类密钥交换协议[12]，其安全性基于 RLWE 问题，进一步将 Peikert 的密钥封装机制集成到了 TSL 中有效证明了协议的可行性。之后的 2016 年 USENIX 安全会议上，Alkim，Ducas，Pöpplemann 和 Schwabe 提出了一个基于 RLWE 的后量子密钥交换方案 NewHope[13]，之后谷歌公司进行了后量子 TLS 实验，在 Chrome 浏览器中部署了 NewHope 方案并进行了运行效率及安全性能测试。不久，Alkim 等人在 NewHope 方案的基础上又提出了一种使用加密机制的被动安全密钥交换协议 NewHope-Simple[14]。该协议在一方通信量上仅增加了 6.25%，在实现分享密钥准确度和有效性不变的情况下，并且未使用计算复杂的调和技术达到了几乎与 NewHope 相同的安全性能。虽然 RLWE 问题环的代数结构使得密钥交换方案具有更为实用的密钥尺寸，可构造更加高效的通信协议，但是 RLWE 问题附加环的代数结构可能存在安全性能上的潜在威胁。2016 年 CCS 大会上，Bos 等人使用 Peikert 错误调和机制的多比特变形提出了一个基于 LWE 问题新型且实用的被动安全密钥交换协议 Frodo[15]，与之前基于 RLWE 问题构造的密钥交换协议相比，虽然计算时间和通信量较大，但安全性能更可靠。

本文主要在 Bos 等人提出的基于 LWE 问题构造的 Frodo 协议的基础上，由 Alkim 等人设计的基于 RLWE 问题使用加密体制的方式构造的 NewHope-Simple 方案得到启示，提出了一种新型高效的基于 LWE 问题被动安全的密钥交换协议，使用了加密机制而未使用计算复杂的错误调和机制，计算简洁高效。该方案仅以一方通信量从 11296 字节增至 11520 字节，大小仅增加 1.09%的微小代价，达到了有效抵御量子攻击同等的安全性能，并使用了 NIST 杂凑函数标准 SHA-3，进一步提高了协议的安全度。与现有的基于 LWE 问题设计的密钥交换协议相比，具有较强的竞争力。

1　基础知识

1.1　带误差学习问题

定义 1　判定性 LWE 问题。已知参数 $n \ge 1$，模数 $q \ge 2$，输入数据为矩阵 $\mathbf{A}$ 和向量 v，已知 $v = \mathbf{A}s + e$，其中 $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$，$s \in \mathbb{Z}_q^n$ 且满足 $\mathbf{A} \xleftarrow{\$} U(\mathbb{Z}_q^{m\times n})$，$s \xleftarrow{\$} U(\mathbb{Z}_q^n)$，即矩阵 $\mathbf{A}$、向量 s 分别在 $\mathbb{Z}_q^{m\times n}$ 和 $\mathbb{Z}_q^n$ 中按照均匀分布随机选择，错误向量 e 在 $\mathbb{Z}_q^m$ 上服从某种公开的概率分布 χ^m，判定性 LWE 问题是指给定 (A,v),区分 (A,v) 为 LWE 分布还是随机选择于均匀分布 $(\mathbb{Z}_q^{m\times n},\mathbb{Z}_q^m)$。

定义 2[15]　$(m,\bar{n})$-矩阵判定性 LWE 问题。已知参数 $n \ge 1$，模数 $q \ge 2$，输入数据为矩阵 $\mathbf{A}$ 和向量 V，已知 $V = \mathbf{A}S + E$，其中 $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$，且满足 $\mathbf{A} \xleftarrow{\$} U(\mathbb{Z}_q^{m\times n})$，即 $\mathbf{A}$ 分别在 $\mathbb{Z}_q^{m\times n}$ 中按照均匀分布随机选择，向量 S、错误向量 E 分别在 $\mathbb{Z}_q^n$ 和 $\mathbb{Z}_q^m$ 上服从某种公开的的概率分布 χ^n、χ^m，$(m,\bar{n})$-矩阵判定性 LWE 问题是指给定 $(\mathbf{A},V)$,区分 $(\mathbf{A},V)$ 为 LWE 分布还是随机选择于均匀分布 $(\mathbb{Z}_q^{m\times n},\mathbb{Z}_q^m)$。

1.2　错误调和机制与一般化错误调和机制

1.2.1 错误调和机制（error reconciliation mechanism）

令 $\lfloor x \rceil = \left\lfloor x + \frac{1}{2} \right\rfloor \in \mathbb{Z}$ 为近似取整函数，定义 $\lfloor x \rceil_p := \lfloor x \cdot \frac{p}{q} \rceil$，$I_0 := \{0,1,\ldots,\lfloor \frac{q}{4} \rceil - 1\}$，$I_1 := \{-\left\lfloor \frac{q}{4} \right\rfloor,\ldots,-1\}$；定义交叉近似函数 $\langle \cdot \rangle_2 : \mathbb{Z}_q \to \mathbb{Z}_2$，具体地，$\langle v \rangle_2 := \left\lfloor \frac{4}{q} \cdot v \right\rfloor \bmod 2$；定义模近似函数

$$\lfloor v \rceil_2 = \begin{cases} 0, & 当 v \in I_0 \cup I_1; \\ 1, & 其他. \end{cases}$$ 。

引理 1[11]　对于偶数 q，如果 $v \in \mathbb{Z}_q$ 是均匀随机的，那么给定 $\langle v \rangle_2$ 时，$\lfloor v \rceil_2$ 在 $\mathbb{Z}_q$ 上也是均匀随机的。令 $E = \left[-\frac{q}{4}, \frac{q}{4} \right)$,则调和函数 $rec : \mathbb{Z}_q \times \mathbb{Z}_2 \to \mathbb{Z}_2$ 定义为

$$rec(w,b) = \begin{cases} 0, & w \in I_1 + E(\mathrm{mod} q); \\ 1, & 其他. \end{cases}$$

引理 2[11]　对于偶数 q,如果 $w = v + e \bmod q$，且 $w \in \mathbb{Z}_q, e \in E$,那么 $rec(w,\langle v \rangle_2) = \lfloor v \rceil_2$。

当 q 为奇数时，为了避免派生未流的不均匀性，引入了随机化函数。令 $dbl : \mathbb{Z}_q \to \mathbb{Z}_{2q}$，$dbl(x) = 2x - \bar{e}$,其中 $\bar{e}$ 为随机项，$\bar{e}$ 为 0 的概率为 $1/2$,e 为 1 和-1 的概率为 $1/2$，从而保证 $\bar{e}$ 在模 2 运算后是均匀的。

引理 3[11]　对于奇数 q,如果 $v \in \mathbb{Z}_q$ 是均匀随机的，令 $\bar{v} = dbl(v) \in \mathbb{Z}_{2q}$，那么在给定 $\langle dbl(v) \rangle_2$ 的情况下，$\lfloor \bar{v} \rceil_2$ 在 $\mathbb{Z}_{2q}$ 上是均匀随机的。令 $E = [-\frac{q}{4}, \frac{q}{4})$，则调和函数 $rec : \mathbb{Z}_{2q} \times \mathbb{Z}_2 \to \mathbb{Z}_2$ 定义为

chinaXiv:201804.02040v1

$$rec(w,b)=\begin{cases}0, & w\in I_1+E(\mathrm{mod}q);\\ 1, & \text{其他.}\end{cases}$$

引理 4[11] 对于奇数 q,令 $v=w+e\in\mathbb{Z}_q$，$w,e\in\mathbb{Z}_q$，且 $2e+\bar{e}\in E \bmod q$，那么 $rec(2w,\langle\bar{v}\rangle)=\lfloor\bar{v}\rceil_2$。

1.2.2 一般化错误调和机制（generalized error reconciliation mechanism）

Peikert 错误调和机制双方仅能通过调和函数 rec 提取 1 比特密钥，一般化错误调和机制是 Peikert 错误调和机制的多比特变形，可保证双方可以通过调和函数 rec 提取 2^B 比特密钥。

已知模数 $q=2^n$，其中 n 为正整数，$B<(\log_2 q)-1$，令 $\bar{B}=(\log_2 q)-B$，对于任意的 $v\in Z_q$，定义近似函数 $\lfloor\cdot\rceil_{2^B}:v\to\lfloor 2^{-\bar{B}}\cdot v\rceil \bmod 2^B$，定义交叉近似函数 $\langle\cdot\rangle_{2^B}:v\to\left\lfloor 2^{-\bar{B}+1}\cdot v\right\rfloor \bmod 2$。

引理 5[15] 如果 $v\in Z_q$ 是均匀随机的，那么给定 $\langle v\rangle_{2^B}$ 时，$\lfloor v\rceil_{2^B}$ 在 Z_q 上也是均匀随机的。

引理 6[15] 如果 $|v-w|<2^{\bar{B}-2}$，那么 $rec(w,\langle v\rangle_{2^B})=\lfloor v\rceil_{2^B}$。

1.3 构造被动安全的 LWE 密钥交换协议的两种方式

基于 LWE 问题构造被动安全密钥交换协议过程中对于针对 LWE 问题其错误向量的处理是需要解决的关键问题，而错误向量的存在是问题困难性的关键，其存在使得通信双方得到近似相等的值。因此，对错误的处理是基于 LWE 问题设计密钥交换协议关键的技术难点。对于错误的处理有两种方式，一种是基于调和机制，一种是基于加密机制。

1.3.1 基于调和机制构造密钥交换协议

Peikert 在 2014 年后量子密码会议上提出了一种高效的基于错误调和机制构造的被动安全密钥封装体制，此技术成为了基于格理论构造认证密钥交换协议的重要基础，后续在 Peikert 错误调和机制的基础上构造了许多高效实用的密钥交换协议。Bos 等人基于 RLWE 问题，使用错误调和机制构造了一个密钥交换协议，图 1 为 BCNS15[12]方案的具体描述。

表 1 基于调和机制构造的密钥交换协议

Alice		Bob
KEM.Setup():		
$a\xleftarrow{\$}R_q$		
Alice		Bob
KEM.Gen(a):		KEM.Encaps(a,b):
$s,e\xleftarrow{\$}\chi$		$s',e',e''\xleftarrow{\$}\chi$
$b\leftarrow as+e$	$\xrightarrow{b}$	$\mu\leftarrow as'+e'$
		$v\leftarrow bs'+e''$
KEM.Decaps $((s,(\mu,c))$:		$\bar{v}\leftarrow dbl(v)\in\mathbb{Z}_{2q}$
$v'\leftarrow 2\mu s$	$\xleftarrow{\mu,c}$	$c\leftarrow\langle\bar{v}\rangle_2$
$\mu\leftarrow \mathrm{Rec}(v',r)$		$\mu\leftarrow\lfloor\bar{v}\rceil_2$

对于 Alice，经计算得到的环元素值为 $v'=\mu s=ass'+e's$，对于 Bob，计算得到的环元素值为 $v=bs'+e''=ass'+es'+e''$，由引理 3 可知，已知 $\langle\bar{v}\rangle_2$ 的情况下，并不会泄露 $\lfloor\bar{v}\rceil_2$ 的任何信息，并且在 $v=w+e$ 时，得到 $rec(2w,\langle\bar{v}\rangle)=\lfloor\bar{v}\rceil_2$。因此，对于 Alice，只需计算 $\mu=rec(2\mu s,r)$，而 Bob 计算 $\mu=\lfloor\bar{v}\rceil_2$，因此 Alice 与 Bob 经过密钥交换得到共享密钥 μ。

1.3.2 基于加密机制构造密钥交换协议

使用错误调和机制构造基于格的密钥交换协议可以有效减少通信量，但是方案的计算复杂。之后的 NewHope-Simple[14]方案和基于模 LWE[19]问题的 Kyber.KE[20]方案均是使用加密机制构造的密钥交换协议。

已知 Alice 和 Bob 有一个共同的系统元素 $a\in R_q$，Alice 从错误分布中取样 (s,e)，计算公钥 $b=as+e$ 给 Bob，Bob 从 χ 中取样 (s',e')，计算 $\mu=as'+e'$、$v=(as+e)s'=ass'+es'$，之后 Alice 根据收到消息计算 $v'=\mu s=(as'+e')s=ass'+e's$，Bob 增加一个噪声项 e''，而 e'' 同样取自 χ，Bob 计算得到 $v''=ass'+es'+e''$，由于 s，s'，e，e' 及 e'' 是很小的量，因此，$v'\approx v''\approx ass'$，这个结论正是基于加密机制构造密钥交换协议的基础。

在 LWE 加密方案中，Bob 通过编码函数将一个秘密消息 v 变成较大的值，$k=Encode(v)$，计算 $c=v+k$，并将 μ、c 发送给 Alice，Alice 计算 $k'=c-v'\approx k$，即恢复了 k 的值，注意，编码函数必须是单射函数，Alice 才能恢复最原始的消息 v。表 2 为基于加密机制构造密钥交换协议的描述。

表 2 基于加密机制构造的密钥交换协议

Alice		Bob
KEM.Setup():		
$a\xleftarrow{\$}R_q$		
Alice		Bob
KEM.Gen(a):		KEM.Encaps(a,b):
$s,e\xleftarrow{\$}\chi$		$s',e',e''\xleftarrow{\$}\chi$
$b\leftarrow as+e$	$\xrightarrow{b}$	$\mu\leftarrow as'+e'$
		$v\leftarrow bs'+e''$
		$\mathrm{v}\xleftarrow{\$}\{0,1\}^n$
		$k\leftarrow Encode(\mathrm{v})$
KEM.Decaps $(s,(\mu,c))$:	$\xleftarrow{\mu,c}$	$c\leftarrow v+k$
$v'\leftarrow\mu s$		$\mu\leftarrow Extract(k)$
$k'\leftarrow c-v'$		
$\mu\leftarrow Extract(k')$		

1.3.3 两种构造方式的优势与劣势

在基于格 LWE 问题设计的密钥交换协议中使用调和机制构造方式可以减少通信量，这正是其优势所在，但是调和机制所使用的调和函数计算相当复杂。使用调和机制构造的密钥交

ChinaXiv合作期刊

换协议主要有基于 RLWE 设计的 NewHope 和基于 LWE 设计的 Frodo。而使用加密机制的构造方式设计的密钥交换协议的优势是在计算上更为简洁高效，但是较之调和机制增加了通信量，为了降低通信量的大小，在加密机制中往往使用密文压缩技术，将密文元素从 $\mathbb{Z}_q$ 映射到 $\mathbb{Z}_p$ 上，其中 $p<q$。密文的低位比特主要是噪声信息，运用密文压缩技术，会使这些信息丢失，但是这些噪声信息的丢失对于恢复其所加密得到的密钥影响并不大。使用加密机制构造的密钥交换协议主要为基于 RLWE 设计的 NewHope-Simple 和基于模 LWE 设计的 Kyber.KE。综上，目前基于 LWE 问题被动安全的密钥交换协议主要基于以上两种机制设计，两种机制有其各自的优势与劣势。

2 基于 LWE 问题的密钥协商协议

2.1 Frodo 密钥交换协议

2016 年 CCS 大会上，Bos 等人提出了基于 LWE 问题的密钥交换协议 Frodo，参数 $n=756$，$q=2^{15}$，χ 是一种抽样效率较高的离散概率密度函数构成的扰动分布，其中 $\bar{m}=\bar{n}=8$，$B=4$。由于 $\bar{m}\cdot\bar{n}\cdot B\geq 256$，这样协议可以达到 128 比特的后量子安全水平。$\bar{m}\cdot\bar{n}$ 是 LWE 问题的维度，B 是双方提取的矩阵每个元素的密钥比特值，B 变大时，$\bar{m}\cdot\bar{n}$ 相应减小，即降低了矩阵的维度，这样可以有效减少带宽，而且可以有效避免 Lojam 攻击。Frodo 方案如表 3 所示。

表 3 Frodo 密钥交换协议

Alice		Bob
$seed_A \xleftarrow{\$} U\left(\{0,1\}^s\right)$		
$\mathbf{A} \leftarrow Gen(\mathrm{seed}_A)$		
$\mathbf{S},\mathbf{E} \xleftarrow{\$} \chi\left(Z_q^{n\times\bar{n}}\right)$		
$\mathbf{B} \leftarrow \mathbf{AS}+\mathbf{E}$	$\xrightarrow[\in\{0,1\}^s\times Z_q^{n\times\bar{n}}]{seed_A,B}$	$\mathbf{A} \leftarrow Gen\left(seed_A\right)$
		$\mathbf{S}',\mathbf{E}' \xleftarrow{\$} \chi\left(Z_q^{\bar{m}\times n}\right)$
		$\mathbf{B}' \leftarrow \mathbf{S}'\mathbf{A}+\mathbf{E}'$
		$\mathbf{E}'' \xleftarrow{\$} \chi\left(Z_q^{\bar{m}\times\bar{n}}\right)$
		$\mathbf{V} \leftarrow \mathbf{S}'\mathbf{B}+\mathbf{E}''$
	$\xleftarrow[\in Z_q^{\bar{m}\times n}\times Z_2^{\bar{m}\times\bar{n}}]{\mathbf{B}',\mathbf{C}}$	$\mathbf{C} \leftarrow \langle\mathbf{V}\rangle_{2^{\mathbf{B}}}$
$K \leftarrow rec\left(\mathbf{B}'\mathbf{S},\mathbf{C}\right)$		$K \leftarrow \lfloor\mathbf{v}\rceil_{2^B}$

2.2 新型密钥交换协议 NewFrodo

Frodo 方案是一个通过一般错误调和机制方式构造的密钥交换协议，这种构造方式虽然高效但计算复杂。本文在 Frodo 方案基础上，基于加密机制构造了一种新型实用的密钥交换协议 NewFrodo。该方案是基于 LWE 构造的可证明被动安全的密钥交换协议，避免使用计算复杂的一般化错误调和机制，并使用 NIST 杂凑函数标准 SHA-3 有效提高了安全性能，可抵御量子攻击，并且计算简洁高效。

该方案中，为有效抵御量子攻击，对参数作如下设置：其中维度 $n=752$，模数 $q=2^{15}$，χ 为抽样效率较高的离散概率密度函数 (PDF) 构成的扰动分布，参数 $\bar{m}=\bar{n}=8$，$B=4$，并且满足 $\bar{m}\cdot\bar{n}\cdot B\geq 256$。具体参数选择参考文献[15]。下面分别为方案中的具体算法。

算法 1 NFEncode 对应函数 $f:K_{Bij}\leftarrow\left\lfloor K_{ij}\cdot\frac{q}{2^B}\right\rfloor$，输入是矩阵 $\mathbf{K}\in\mathbb{Z}_{2^B}^{\bar{m}\times\bar{n}}$，矩阵元素为 K_{ij}，$0\leq i\leq\bar{m}-1, 0\leq j\leq\bar{n}-1$，输出是矩阵 $\mathbf{K_B}\in\mathbb{Z}_q^{\bar{m}\times\bar{n}}$，矩阵元素为 K_{Bij}，$0\leq i\leq\bar{m}-1$，$0\leq j\leq\bar{n}-1$；

算法 2 NFDecode 对应函数 $f:K_{Aij}\leftarrow\left\lfloor K_{ij}\cdot\frac{2^B}{q}\right\rfloor$，输入是矩阵 $\mathbf{K_A}\in\mathbb{Z}_q^{\bar{m}\times\bar{n}}$，矩阵元素为 K_{Aij}，$0\leq i\leq\bar{m}-1$，$0\leq j\leq\bar{n}-1$，输出是矩阵 $\mathbf{K}'\in\mathbb{Z}_{2^B}^{\bar{m}\times\bar{n}}$，矩阵元素为 K'_{ij}，$0\leq i\leq\bar{m}-1$，$0\leq j\leq\bar{n}-1$；

算法 3 $tran^1$ 为字符串转换为矩阵，对应函数 $f:K_{ij}\leftarrow\{v'_{4k},v'_{4k+1},v'_{4k+2},v'_{4k+3}\}, 0\leq k\leq 64$，输入是字符串 $v'\in\{0,1\}^{256}$，$\{v_{4k},v_{4k+1},v_{4k+2},v_{4k+3}\}, 0\leq k\leq 64$，输出是矩阵 $\mathbf{K}\in\mathbb{Z}_{2^B}^{\bar{m}\times\bar{n}}$，$B=4$，矩阵元素为 K_{ij}，$0\leq i\leq\bar{m}-1$，$0\leq j\leq\bar{n}-1$；

算法 4：$trans^2$ 为矩阵转换为字符串，对应函数 $f:\{v'_{4k},v'_{4k+1},v'_{4k+2},v'_{4k+3}\}\leftarrow K'_{ij}, 0\leq k\leq 64$，输入是矩阵 $\mathbf{K}'\in\mathbb{Z}_{2^B}^{\bar{m}\times\bar{n}}$，$B=4$，矩阵元素为 K'_{ij}，$0\leq i\leq\bar{m}-1$，$0\leq j\leq\bar{n}-1$，输出是字符串 $v''\in\{0,1\}^{256}$，$\{v''_{4k},v''_{4k+1},v''_{4k+2},v''_{4k+3}\}, 0\leq k\leq 64$。

下面是方案的具体执行过程：

a）首先 Alice 从 $\{0,1\}^s$ 随机均匀抽样，得到密钥种子 $seed_A$，通过 Gen 函数形成矩阵 $\mathbf{A}\in Z_q^{n\times n}$，从噪声分布 χ 中随机均匀抽样得到矩阵 $\mathbf{S},\mathbf{E}\in\mathbb{Z}_q^{n\times\bar{n}}$，Alice 计算 $\mathbf{B}=\mathbf{AS}+\mathbf{E}$ 得到矩阵 $\mathbf{B},\mathbf{B}\in Z_q^{n\times\bar{n}}$，Alice 将 $seed_A,\mathbf{B}$ 发送至 Bob;

b）Bob 同样利用 $seed_A$ 产生相同的矩阵 $\mathbf{A}\in\mathbb{Z}_q^{n\times n}$，从噪声分布 χ 中随机均匀抽样得到矩阵 $\mathbf{S}',\mathbf{E}'\in\mathbb{Z}_q^{\bar{m}\times n}$，Bob 计算 $\mathbf{B}'=\mathbf{S}'\mathbf{A}+\mathbf{E}'$，$\mathbf{B}'\in\mathbb{Z}_q^{\bar{m}\times n}$。从噪声分布 χ 中随机均匀抽样得到矩阵 $\mathbf{E}''\in\mathbb{Z}_q^{\bar{m}\times\bar{n}}$，$v$ 是一段长度为 256 比特的 $\{0,1\}$ 字符串，使用 $SHA3-256$ 得到字符串 v'，再经过 $trans^1$ 将字符串转变为 $\bar{m}\times\bar{n}$ 的矩阵 $\mathbf{K}$，且矩阵中的每个元素 $K_i\in\mathbb{Z}_{2^B}$，对矩阵 $\mathbf{K}$ 由 $NFEncode$ 函数得到矩阵 $\mathbf{K}_B$，Bob 计算 $\mathbf{C}=\mathbf{S}'\mathbf{B}+\mathbf{E}''+\mathbf{K_B}$，发送矩阵 $\mathbf{B}'$、$\mathbf{C}$ 给 Alice。Bob 对 v' 使用 SHA3-256 得到共享密钥 SK_B；

c)Alice 计算 $\mathbf{K_A}=\mathbf{C}-\mathbf{B}'\mathbf{S}$，$\mathbf{K_A}\in\mathbb{Z}_q^{\bar{m}\times\bar{n}}$，$\mathbf{K_A}$ 由 $NFDecode$ 得到矩阵 $\mathbf{K}'$，$\mathbf{K}'$ 经过 $trans^2$ 由矩阵转变为长度为 $\bar{m}\cdot\bar{n}\cdot B$ 的字

chinaXiv:201804.02040v1

ChinaXiv合作期刊

符串 v''，Alice 对字符串 v'' 使用 SHA3-256 得到共享密钥 SK_A。

由上述方案，由双方的传输消息进行方案的相关正确性分析：将 Bob 计算量 $\mathbf{C}=\mathbf{S}'\mathbf{B}+\mathbf{E}''+\mathbf{K_B}$ 代入 Alice 计算式 $\mathbf{K_A}=\mathbf{C}-\mathbf{B}'\mathbf{S}=\mathbf{S}'\mathbf{B}+\mathbf{E}''+\mathbf{K_B}-\mathbf{B}'\mathbf{S}=\mathbf{S}'(\mathbf{AS}+\mathbf{E})+\mathbf{E}''+\mathbf{K_B}-(\mathbf{S}'\mathbf{A}+\mathbf{E}')\mathbf{S}$，由于 $\mathbf{E}$，$\mathbf{E}'$，$\mathbf{E}''$ 是很小的量，因此可得 $\mathbf{K_A}=\mathbf{C}-\mathbf{B}'\mathbf{S}\simeq\mathbf{K_B}$。由 *NFEncode*，*NFDecode* 可得 $\mathbf{K}'\approx\mathbf{K}$，进而可得 $SK_A=SK_B=SK$。

表 4 本文设计方案

Alice		Bob
$seed_A \xleftarrow{\$} U(\{0,1\}^s)$		
$\mathbf{A}\leftarrow Gen(\text{seed}_A)$		
$\mathbf{S},\mathbf{E}\xleftarrow{\$}\chi(\mathbb{Z}_q^{n\times\bar{n}})$		
$\mathbf{B}\leftarrow\mathbf{AS}+\mathbf{E}$	$\xrightarrow[\in\{0,1\}^s\times Z_q^{n\times\bar{n}}]{seed_A,\mathbf{B}}$	$\mathbf{A}\leftarrow Gen(seed_A)$
		$\mathbf{S}',\mathbf{E}'\xleftarrow{\$}\chi(\mathbb{Z}_q^{\bar{m}\times n})$
		$\mathbf{B}'\leftarrow\mathbf{S}'\mathbf{A}+\mathbf{E}'$
		$\mathbf{E}''\xleftarrow{\$}\chi(\mathbb{Z}_q^{\bar{m}\times\bar{n}})$
		$v\xleftarrow{\$}\{0,1\}^{256}$
		$v'\leftarrow SHA3-256(v)$
		$\mathbf{K}\leftarrow trans^1(v')$
		$\mathbf{K_B}\leftarrow NFEconde(\mathbf{K})$
$\mathbf{K_A}\leftarrow\mathbf{C}-\mathbf{B}'\mathbf{S}$	$\xleftarrow[\in Z_q^{\bar{m}\times n}\times Z_q^{\bar{m}\times\bar{n}}]{\mathbf{B}',\mathbf{C}}$	$\mathbf{C}\leftarrow\mathbf{S}'\mathbf{B}+\mathbf{E}''+\mathbf{K_B}$
$\mathbf{K}'\leftarrow NFDecode(\mathbf{K_A})$		$SK_B\leftarrow SHA3-256(v')$
$v''\leftarrow trans^2(\mathbf{K}')$		
$SK_A\leftarrow SHA3-256(v'')$		

3 安全性分析

本文协议被动攻击下可证明安全，首先通信报文不泄露关于秘密的信息，其次需证明双方交换的密钥与随机数不可区分。考虑敌手 M 尝试在给定密钥交换协议中区分会话密钥 SK 和均匀随机密钥 SK'，定义敌手 M 赢得游戏的优势为

$$Adv_{n,\bar{n},\bar{m},B,q,\chi}^{ddh-like}(M)=\left|\Pr\left[M(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},SK)=1\right]-\Pr\left[M(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},SK')=1\right]\right|.$$

定理 1 令 $n,\bar{n},\bar{m},B$ 和 q 是有效整数，χ 是 Z_q 上一特定错误分布，如果 Gen 是一个安全的伪随机函数，并且设置参数为 (n,q,χ)，此时判定性 LWE 问题是困难的，即本文提出的密钥交换协议产生的密钥是难以区分的，即

$$Adv_{n,\bar{n},\bar{m},B,q,\chi}^{ddh-like}(M)\le Adv_{Gen}^{\Pr f}(B_0)+\bar{n}\cdot Adv_{n,q,\chi}^{dlwe}(M\cdot B)+\bar{m}\cdot Adv_{n,q,\chi}^{dlwe}(M\cdot B_2)$$

表 5 为 B_1，B_2 算法的具体流程，B_0 隐含在证明中。

表 5 算法的具体流程

$B_1(\mathbf{A},\mathbf{B})$:	$B_2(\mathbf{Y},\mathbf{Z})$:
1.$\mathbf{S}',\mathbf{E}'\xleftarrow{\$}\chi(\mathbb{Z}_q^{\bar{m}\times\bar{n}})$	1.$\begin{pmatrix}\mathbf{A}^T\\\mathbf{B}^T\end{pmatrix}\leftarrow Y$
2.$\mathbf{B}'\leftarrow\mathbf{S}'\mathbf{A}+\mathbf{E}'$	2.$v\xleftarrow{\$}\{0,1\}^{256}$
3.$\mathbf{E}''\xleftarrow{\$}\chi(\mathbb{Z}_q^{\bar{m}\times\bar{n}})$	3.$v'\leftarrow SHA3-256(v)$
4.$v\xleftarrow{\$}\{0,1\}^{256}$	4.$\begin{pmatrix}\mathbf{B}'^T\\\mathbf{C}^T\end{pmatrix}\leftarrow\mathbf{Z}$
5.$v'\leftarrow SHA3-256(v)$	5.$\mathbf{K_A}\leftarrow\mathbf{C}-\mathbf{B}'\mathbf{S}$
6.$\mathbf{K}\leftarrow trans^1(v')$	6.$SK\leftarrow SHA3-256(v')$
7.$\mathbf{K_B}\leftarrow NFEncode(\mathbf{K})$	7.$SK'\xleftarrow{\$}U(\{0,1\}^{\bar{n}\cdot\bar{m}\cdot B})$
8.$\mathbf{C}\leftarrow\mathbf{S}'\mathbf{B}+\mathbf{E}''+\mathbf{K_B}$	8.$b^*\xleftarrow{\$}(\{0,1\})$
9.$\mathbf{K_A}\leftarrow\mathbf{C}-\mathbf{B}'\mathbf{S}$	9.如果 $b^*=0$，返回 (A,B,B',C,SK)
10.$SK\leftarrow SHA3-256(v')$	10.否则返回 (A,B,B',C,SK')
11.$SK'\xleftarrow{\$}U(\{0,1\}^{\bar{n}\cdot\bar{m}\cdot B})$	
12.$b^*\xleftarrow{\$}U(\{0,1\})$	
13.如果 $b^*=0$，返回 (A,B,B',C,SK)	
14.否则返回 (A,B,B',C,SK')	

证明 在下述游戏证明中，S_i 表示在 $Game_i$ 中表示敌手猜测 b^* 的值，$b^*\in\{0,1\}$。

$Game_0$. 消息是由本文协议真实产生的。以下均是 LWE 分布实例，$(\mathbf{A},\mathbf{B})$ 包含秘密值 $\mathbf{S}$，$(\mathbf{A},\mathbf{B}')$ 与 $(\mathbf{B},\mathbf{V})$ 包含秘密值 $\mathbf{S}'$，因此

$$Adv_{n,\bar{n},\bar{m},B,q,\chi}^{ddh-like}(M)=\left|\Pr(S_0)-\frac{1}{2}\right| \quad (1)$$

$Game_1$. 公钥矩阵 $\mathbf{A}$ 是随机均匀产生的，而不是使用 Gen 函数，由 $seed_A$ 伪随机产生的。

$Game_0$ 与 $Game_1$ 的区别：敌手 M 可以区分这两个游戏，则需要一个区分器 B_0，B_1

$$\left|\Pr(S_0)-\Pr(S_1)\right|\le Adv_{Gen}^{\Pr f}(B_0) \quad (2)$$

$Game_2$. Alice 的临时公钥 $\mathbf{B}$ 是随机均匀产生的，而非从 $(n,\bar{n})-$ 矩阵的判定性 LWE 问题实例中产生，LWE 分布实例 $(\mathbf{A},\mathbf{B}')$ 和 $(\mathbf{B},\mathbf{C})$ 都有秘密矩阵 $\mathbf{S}'$。

$Game_1$ 与 $Game_2$ 的区别：在 $Game_1$ 中，$(\mathbf{A},\mathbf{B})$ 是 $O_{x,s}$ 分布的一个样本，在参数为 (n,q,χ) 的判定性 LWE 问题的假设下，这两种分布是难以区分的。

更准确地说，图 5 中的算法 B_1 的输入为 $(\mathbf{A},\mathbf{B})$，若 $(\mathbf{A},\mathbf{B})$ 是 $O_{x,s}$ 分布的一个样本，并且满足 $\mathbf{S}\xleftarrow{\$}\chi(Z_q^{n\times\bar{n}})$，则 B_1 的输与 $Game_1$ 输出相同，若 $(\mathbf{A},\mathbf{B})$ 是 $U(\mathbb{Z}_q^{n\times\bar{n}})\times U(\mathbb{Z}_q^{n\times\bar{n}})$ 分布的一个样本，则的输出与 $Game_2$ 的输出相同，输出 B_1 与 $Game_2$ 相同。如果敌手 M 可以区分 $Game_1$ 和 $Game_2$，那么 $M\cdot B_1$ 可以区分 $O_{x,s}$ 分布和 $U(Z_q^{n\times\bar{n}})\times U(Z_q^{n\times\bar{n}})$ 分布。因此，

chinaXiv:201804.02040v1

ChinaXiv合作期刊

chinaXiv:201804.02040v1

$$\left|\Pr(S_1)-\Pr(S_2)\right|\le \bar{n}\cdot Adv_{n,q,\chi}^{dlwe-ss}(M\cdot B_1). \qquad (3)$$

$Game_3$. Bob 的临时公钥 $\mathbf{B}'$ 和矩阵 $\mathbf{C}$ 同时由 $\mathbf{S}'$ 产生，在 $Game_3$ 中，包含秘密值 $\mathbf{S}'^{\mathrm{T}}$ 的 $\left\{\begin{pmatrix}\mathbf{A}^{\mathrm{T}}\\ \mathbf{B}^{\mathrm{T}}\end{pmatrix},\begin{pmatrix}\mathbf{B}'^{\mathrm{T}}\\ \mathbf{C}^{\mathrm{T}}\end{pmatrix}\right\}$ 是 $(n+\bar{n},\bar{m})-$ 矩阵判定性 LWE 问题的一个实例。

$Game_2$ 与 $Game_3$ 的区别。由分析可知

$$\mathbf{Pr}(\mathbf{S}_1)=\mathbf{Pr}(\mathbf{S}_2) \qquad (4)$$

$Game_4$. Bob 的临时公钥 $\mathbf{B}'$ 和矩阵 $\mathbf{C}$ 均是随机均匀产生的,而不是同时从 $\mathbf{S}'$ 中产生的。

$Game_3$ 与 $Game_4$ 的区别。在 $Game_3$ 中，$([\mathbf{A}\|\mathbf{B}],[\mathbf{B}'\|\mathbf{C}])$ 是 $(n+\bar{n},\bar{m})-$ 矩阵判定性 LWE 问题的随机 $O_{\chi,s'}$ 分布的一个样本。在 $Game_4$ 中，$([\mathbf{A}\|\mathbf{B}],[\mathbf{B}'\|\mathbf{C}])$ 是 $\mathcal{U}(\mathbb{Z}_q^{(n+\bar{n})\times n})\times\mathcal{U}(\mathbb{Z}_q^{(n+\bar{n})\times m})$ 的一个样本。设置参数为 (n,q,χ)，在判定性 LWE 问题的假设下，这两种分布是难以区分的。更准确地说，图 5 所示的 B_2 算法将 $(\mathbf{Y},\mathbf{Z})\in\mathbb{Z}_q^{(n+\bar{n})\times n}$ 作为输入，若 $(\mathbf{Y},\mathbf{Z})$ 是 $(n+\bar{n},\bar{m})-$ 矩阵判定性 LWE 问题的随机 $O_{\chi,s'}$ 分布的一个样本，且满足 $\mathbf{S}\xleftarrow{\$}\chi(\mathbb{Z}_q^{n\times\bar{n}})$，则 B_2 的输出与 $Game_3$ 输出相同，若 $(\mathbf{A},\mathbf{B})$ 是 $\mathcal{U}(\mathbb{Z}_q^{n\times\bar{n}})\times\mathcal{U}(\mathbb{Z}_q^{n\times\bar{n}})$ 分布的一个样本，则 B_2 的输出与 $Game_4$ 的输出相同。如果敌手 M 可以区分 $Game_3$ 和 $Game_4$，那么 $M\cdot B_2$ 可以区分 $O_{\chi,s'}$ 和 $\mathcal{U}(\mathbb{Z}_q^{(n+\bar{n})\times n})\times\mathcal{U}(\mathbb{Z}_q^{n\times\bar{m}})$ 这两种分布的样本。因此，

$$\left|\Pr(S_3)-\Pr(S_4)\right|\le \bar{m}\cdot Adv_{n,q,\chi}^{ddh-like}(M\circ B_2). \qquad (5)$$

$Game_4$ 的分析.敌手 M 猜测 b^* 的值从而来区分 SK 和 SK'，在 $Game_4$ 中，SK' 是从 $\{0,1\}^{\bar{m}\cdot\bar{n}\cdot B}$ 中随机均匀产生的，敌手 M 已知矩阵 $\mathbf{C}$，在给定 $\mathbf{C}$ 的情况下，$\mathbf{K_A}$ 是随机均匀的，进而可得 $\mathbf{SK}$ 也是随机均匀的，因此，敌手 M 无法得到 b^* 的任何信息，可得

$$\Pr(\mathrm{S}_4)=\frac{1}{2} \qquad (6)$$

综合等式（1）~（6），定理 1 得证。

本文提出的基于 LWE 问题构造的密钥交换协议 NewFrodo，根据 Regev 给出的格最坏情况困难问题到 LWE 问题的归约结论，该协议的安全性最终可以基于格下标准最坏情况困难假设。因此，本文提出的密钥交换协议在被动攻击下可证明安全。

4 效率分析

通过目前公开的学术文献，对现有的基于 LWE 问题来构造的被动安全的密钥交换协议进行综合分析。为了说明方案的优劣，选取最典型的 BCNS15[12]、Newhope、NewHope-Simple、Frodo 四个方案，通过密钥交换协议方案的参数设置、困难问题假设、使用的 KEM 方式、消息长度等方面，进行对比以便突显本方案综合性能。表 1 是本方案与现有的基于 RLWE、LWE 的密钥交换方案进行对比。

BCNS15 方案选取的参数为维度 n=1024，模数 q= $2^{32}-1$，错误分布是离散高斯分布且方差为 $4\sqrt{2}/\pi$ 。在该参数的设置下，最终生成共享会话密钥失败的概率很低，后量子安全性约为 80 比特。该方案通信双发最终可生成 1024 比特大小的共享密钥，但在实际需求中仅需 256 比特；2015 年，Akim 等人全面提升了 BCNS15 协议，提出了一种基于 RLWE 问题的协议 NewHope 密钥交换协议，在参数设置方面采用了相同的维度 n，模数 q=12289，错误分布为中心二项分布。方差为 8，在该参数的设置下，使得生成共享密钥失败的概率可以忽略，并且后量子安全性达到了 206 比特。选取中心二项分布代替原来的离散高斯分布，大大提高了协议的计算效率；2016 年 Akim 等人提出了基于加密机制构造的协议 NewHope-Simple，参数设置包括维度 n，模数 q 以及错误分布与方差均相同。通信量与 NewHope 相比只增加了 6.25%，但是方案未使用计算复杂的调和技术，协议更加简洁高效。由于参数设置相同，因此共享密钥失败概率几乎相等，且后量子安全性相同均为 206 比特；由于 RLWE 问题其环上特殊的代数结构存在安全性的潜在威胁，2016 年 CCS 安全会议上 Bos 等人基于 LWE 问题使用调和机制构造了一种密钥交换协议 Frodo，根据推荐参数，维度 n=756，模数 q= 2^{15}，错误分布为抽样效率更高的离散概率密度（PDF）函数构成的扰动分布，方差为 1.75，由于协议使用了更一般的调和机制，在每次执行 rec 函数时可以得到 4 比特数据，使得生成共享密钥失败的概率增加，但在参数设置下，使得失败概率依然可以忽略，且该方案后量子安全性达到了 130 比特。

本方案与基于 LWE 问题构造的 Frodo 协议相比，以一方通信量从 11 296 Byte 增至 11 520 Byte,仅增加 1.09%的微小代价，避免使用计算复杂的调和机制而使用计算简单的加密机制，方案计算更加简洁高效，并使用了 NIST 杂凑函数标准 SHA-3，进一步提高了协议的安全度。参数设置与 Frodo 方案相同，因此协议失败概率也可忽略，后量子安全性也达到 130 bit。且该协议在被动攻击下可证明安全，可有效抵御量子攻击。

5 结束语

本文设计了一种基于格上 LWE 问题的被动安全的密钥交换协议，结合 Bos 等人提出的被动安全的密钥交换协议 Frodo 以及 Alkim 等人提出的密钥交换协议 NewHope-Simple 的突出优势。Frodo 协议使用调和机制，虽然通信量较小，但错误调和机制 rec 函数计算复杂，本文方案正是避免使用错误调和机制而借鉴了 NewHope-Simple 中的基于加密机制的构造方式，使

ChinaXiv合作期刊

得计算更加简洁高效。与基于 RLWE 问题构造的密钥交换协议相比，虽然密钥尺寸较大，但 RLWE 问题附加环的代数结构存在潜在的安全性威胁，基于 LWE 问题较之 RLWE 问题设计的密钥交换协议在安全性能上更加稳健。最近，Bos 等人提出了一种基于模 LWE 问题的高效安全的密钥交换协议 Kyber.KE[20]。下一步考虑基于 LWE 问题、RLWE 问题及模 LWE 问题设计出更加实用、高效的密钥交换协议。

表 1 基于 RLWE 与 LWE 的密钥交换协议的性能比较

方案	维度 n	模数 q	错误分布 χ、方差 σ^2	困难假设	构造方式	通信计算复杂度	通信量（byte） $A\to B$	通信量（byte） $B\to A$	后量子安全(bit)
BCNS15	1024	$2^{32}-1$	高斯分布、$4\sqrt{2}/\pi$	RLWE	调和机制	$n+2n\log_2 q$	4096	4224	80
NewHope	1024	12289	二项分布、8	RLWE	调和机制	$2n+2n\log_2 q$	1824	2048	206
NewHope-Simple	1024	12289	二项分布、8	RLWE	加密机制	$3n+2n\log_2 q$	1824	2176	206
Frodo	756	2^{15}	PDF 扰动分布、1.75	LWE	调和机制	$(\bar{n}+\bar{m})(n\log_2 q+1)$	11377	11296	130
本方案	756	2^{15}	PDF 扰动分布、1.75	LWE	加密机制	$(\bar{n}+\bar{m})(n\log_2 q+4)$	11377	11520	130

参考文献：

[1] Dodis Y, Mironov I, Stephens-Davidowitz N. Message transmission with reverse firewalls-secure communication on corrupted machines [C]// Advances in Cryptology-CRYPTO. Berlin: Springer, 2016: 341-372.

[2] Benzvi A, Blackburn S R, Tsaban B. A practical cryptanalysis of the algebraic eraser [C]// Advances in Cryptology-CRYPTO. Berlin: Springer, 2016: 179-189.

[3] Diffie W, Hellman M. New directions in cryptography [J]. IEEE Trans on Information Theory, 1976, 22 (6): 644-654.

[4] Chen L, Jordan S, et al. Report on post-quantum cryptography [M]. Gaithersburg: National Institute of Standards and Technology, 2016.

[5] Gorbunov S, Vaikuntanathan V, Wee H. Predicate encryption for circuits from LWE [C]// Proc of CRYPTO. Berlin: Springer, 2015: 503-523.

[6] Gorbunov S, Vaikuntanathan V, Wee H. Attribute-based encryption for circuits [C]// Proc of ACM Symp on Theory of Computing. NewYork: ACM Press, 2013: 545-554.

[7] Boneh D, Gentry C, Gorbunov S, et al. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits [C]// Proc of EUROCRYPT. Berlin: Springer, 2014: 533-556.

[8] Bai S, Galbraith S D. An improved compression technique for signature based on learning with errors [C]// Proc of Topics in Cryptology. Berlin: Springer, 2014: 28-47.

[9] Lyubashevsky V. Digital signatures based on the hardness of ideal lattice problems in all rings [C]// Proc of ASIACRPT. Berlin: Springer, 2016: 196-214.

[10] Ding J, Universuty C. A simple provably secure key exchange scheme based on the learning with errors problem [J]. IACR Cryptology ePrint Archive, 2012.

[11] Peikert C. Lattice cryptography for the Internet [C]// Post-QuantumCryptography. Berlin: Springer, 2014. 197-219.

[12] Bos J W, Costello C, Naehrig M, Stebila D. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem [C]// Proc of IEEE Symposium on Security and Privacy, Washington DC: IEEE Computer Society Press, May 2015: 553-570.

[13] Alkim E, Pöpplemann D, Schwabe P. Post-quantum key exchange: a new hope [C]// USENIX Security 16. [S. l.] : USENIX Association, 2015.

[14] Alkim E, Pöpplemann D, Schwabe P. NewHope without reconciliation [J]. IACR Cryptology ePrint Archive, 2016, 2016: 1157.

[15] Bos J, Costello C, et al. Frodo!take off the ring!practical, quantum secure key exchange from LWE [C]// Proc of Conference on Computer and Communications Security. New York: ACM Press, 2016: 1006-1018.

[16] Benhamouda F, Camenisch J, Krenn S, et al. Better zero-knowledge proofs for lattice encryption and their application to group signatures [C]// Proc of ASIACRYPT. Berlin: Springer, 2014: 551-572.

[17] Regev O. On lattices, learning with errors, random linear codes, and cryptography [J]. Journal of the ACM, 2005, 56 (6): 84-93.

[18] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings [C]// Advance in EuroCrypt. Berlin: Springer, 2010: 1-23.

[19] Langlois A, Stehlé D. Worst-case to average-case reductions for module lattices [J]. Designs, Codes and Cryptography, 2015, 75 (3): 565–599.

[20] Bos J, Ducas L, Kiltz E, et al. Crystals-Kyber: a CCA-secure module-lattice-based KEM [J]. IACR Cryptology ePrint Archive, 2017, 2017: 634.

chinaXiv:201804.02040v1